NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1600.1
Effective Date:
November 03, 2004
Expiration Date:
November 03, 2014

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Security Program Procedural Requirements w/Change 2 (4/01/2009)

Responsible Office: Office of Protective Services

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

Chapter 10: Glossary of Terms, Abbreviations, and Acronyms

Access - Used under two separate and distinct contexts within this NPR:

(1). The ability, opportunity, and authority, to gain knowledge of classified information or gain authorized entry onto a NASA classified IT resource. (Refer to Chapters 2 and 6), or;

(2). The act of obtaining authorized physical entry onto a NASA Installation, facility, or unclassified NASA IT resource (Refer to Chapters 3 and 4).

Access Control System - Electromechanical and electronic devices that monitor and permit or deny entry and exit of a protected area by personnel or vehicles.

Accreditation - Formal declaration by a Designated Approving Authority (DAA) that an information technology system is approved to operate in a particular security mode for the purpose of processing CNSI, using a prescribed set of safeguards. Accreditation Authority is synonymous with DAA.

ACI (Administratively Controlled Information) - Official NASA or other government information and material, of a sensitive but unclassified nature, which does not contain National security information (and therefore cannot be classified), nonetheless, must still be protected against unauthorized disclosure.

Adjudication - A fair and logical Agency determination, based upon established adjudicative guidelines and sufficient investigative information, as to whether or not an individual's access to classified information, suitability for employment with the U.S. Government, or access to NASA facilities, information, or IT resources, is in the best interest of National security or efficiency of the Government.

Administrative Downgrade - A determination that an individual's level of access to classified information requires reduction or removal based solely upon a change in the individual's "Need to Know." It is not an adverse action.

Adverse Impact - An act or occurrence that results in a negative outcome and/or damage of an asset, program, mission, or operation thereby delaying or interrupting performance for a specified short period of time.

Arrest Authority - The power to execute arrests, without a warrant, and to conduct searches incident to an arrest, granted to designated NASA Security Officials and Security Services Contractors, pursuant to Section 104(f) of the National Aeronautics and Space Act of 1958, as amended, and 14 CFR Part 1203b.

Asset - A system, object, person, or any combination thereof, that has importance or value; includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources.

Asset Value - The established worth of a particular asset or resource. May be assessed relative to: monetary value, current replacement value, historic value, political value, prestige, or a combination.

Background Investigation (BI) - The BI consists of a Personal Subject Interview, a basic National Agency Check (NAC) including credit search, personal interviews with employment, residence (neighbors), educational sources, and law enforcement searches. Total coverage is for a 5-year period. A BI is required for all High Risk positions.

Baseline Physical Security Posture - An initial determination, based on a physical security vulnerability assessment that describes the Center's existing security posture, from which the CCS can recommend or require adjustments in order to bring the security posture up to minimum standards, if necessary.

Center Chief of Security (CCS) - The senior Center security official responsible for management of the Center security program.

Central Adjudication Facility (NASA CAF) - Facility established at the DSMD level responsible for adjudicating all requests for clearances to access CNSI.

Certifying Authority (CA) - Individual responsible for ensuring and certifying, to the DAA, that requisite security measures are implemented for IT Systems identified for processing of classified information.

Certifying Officials - The AA/OSPP, DSMD, Center Directors, or the Center Chief of Security who are, by virtue of this NPR, authorized to certify that an individual has met established requirements (training, firearms qualification, etc.), can perform those security functions designated in their position description, and can carry a firearm in performance of their security duties. They can also approve the use of a security room, vault, or container for storage of CNSI.

Certification - Used under two separate contexts in this NPR:

(1) A formal process used by the Certifying Official to ensure that an individual has met all established training requirements as necessary to perform their security responsibilities.

(2) A formal process implemented at the CCS level to ensure a room, vault, or security container meets minimum structural and physical security attributes necessary to ensure adequate protection of CNSI. Certified Tempest Technical Authority (CTTA) - Designated official responsible for performing Tempest countermeasures cost and security analyses prior to the implementation of Tempest countermeasures.

Classification Category - The specific degree of security classification that has been assigned to CNSI to indicate the extent of protection required in the national interest:

(1) **Confidential** - Information, the unauthorized disclosure of which reasonably could be expected to cause damage to National security that the Original Classification Authority (OCA) is able to identify or describe.

(2) **Secret** - Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to National security that the OCA is able to identify or describe.

(3) **Top Secret** - Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to National security that the OCA is able to identify or describe.

Classification Guide - The written direction issued or approved by a Top Secret Original Classification Authority (TS/OCA) that identifies the information or material to be protected from unauthorized disclosure and specifies the level and duration of classification assigned or assignable to such information or material.

Classified National Security Information (CNSI) - Information that must be protected against unauthorized disclosure IAW Executive Order (EO) 12958, "Classified National Security Information," as amended, and is marked to indicate its classified status when in documentary form. See definition for "Classification Category" above.

Classified Material - Any physical object on which is recorded, or in which is embodied, CNSI that shall be discerned by the study, analysis, observation, or other use of the object itself.

Cleared Person - An individual who has been granted a security clearance making them eligible to access CNSI up to and including the cleared level.

Closed Area - A space in which security measures are applied primarily to safeguard CNSI and material with entry to that space being equivalent to access to such classified information and material.

Competent NASA Medical Authority - A NASA civil service or contract physician responsible for reviewing medical records, providing results of medical evaluations, and interpreting evaluations as they relate to reliable performance of duties for the NASA Mission Critical Space Systems Personnel Reliability Program.

Component Facilities - NASA-owned facilities not located on any NASA Center (e.g., Michoud Assembly Facility, Wallops Flight Facility, White Sands Test Facility, NASA

IV&V).

Compromise - The improper or unauthorized disclosure of or access to classified information.

Communications Security (COMSEC) - The protection resulting from the application of crypto security, transmission security, and emission security measures to telecommunications and from the application of physical security measures to COMSEC information. These measures are taken to deny unauthorized persons information of value that might be derived from the possession and study of such telecommunications or to ensure the authenticity of such telecommunications.

Continuous Evaluation Program (CEP) - A process, established under this NPR, to ensure personnel employed by NASA or its contractors maintain eligibility for employment and access to CNSI, NASA facilities, information, and resources.

Contractor - For the purpose of this NPR, any non-NASA entity or individual working on a NASA installation or accessing NASA information technology.

Counterintelligence - Information gathered and activities conducted to protect against espionage and sabotage and other intelligence activities conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document, or communications security.

Credit Searches - Credit searches are conducted as part of the Minimum Background Investigation (MBI), Limited Background Investigation (LBI), Background Investigation (BI), Single Scope Background Investigation (SBI), Periodic Reinvestigation (PRI), Upgrade, and Update cases. Credit searches shall be conducted in conjunction with a National Agency Check and Inquiries (NACI) upon initial entry of duty (EOD) for all appointees and as needed to review the suitability of an employee who is moving from a low or moderate risk position to a high risk position. Credit searches shall also be completed upon reinstatement or transfer of a federal employee whose BI is otherwise in order. Credit searches are not routinely performed on current employees.

Amendments to the Fair Credit Reporting Act (FCRA) (15 U.S.C. - 1681, et seq) address permissible purposes for which consumer reports may be furnished and conditions for furnishing and using consumer reports for employment purposes. Subsection 1681b (b)(2) of Title 15 requires that the applicant/employee must authorize this use in writing before the consumer report is obtained.

Subsection 1681b (b)(3) of Title 15 requires that, before taking an action adverse to the employee or applicant for employment based in whole or in part on a consumer report, the agency must notify the consumer of the proposed negative action and provide the consumer with a copy of the report and a copy of the Federal Trades Commission's (FTC) Consumer Rights Notice.

Critical-Sensitive (CS) (EO 10450) - One of the three levels for designating National security-related positions and the degree of risk involved. Includes any position involving access to TOP Secret information; investigative requirements for this position are covered under NSD-61.

Critical Infrastructure - Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Public Law 107-56, U.S. Patriot Act Section

1016 (e))

Cryptographic Information - All data and material, including documents, devices, equipment and apparatus, essential to the encryption, decryption, or authentication of telecommunications. Whenever such cryptographic information is classified, the material is marked "CRYPTO," and the specific security classification is indicated.

Custodian (Classified Material) - Any authorized person who possesses the appropriate security clearance and is in possession of and responsible for safeguarding classified information or material.

Deadly Force - A degree of force that a reasonable person would consider likely to cause death or serious bodily harm.

Debarment - Official determination made in writing by the Center Director or Center Chief of Security that bars, for cause, an individual from accessing NASA property.

Decertification - Used in the context of rooms, vaults, or security containers designated for approved storage of classified material. Indicates a formal process developed and implemented to remove a room, vault, or security container from the Center inventory of approved CNSI storage mediums.

Declassification - The authorized change in the status of information from classified information to unclassified information.

Denial - The adjudication that an individual's initial access to classified information would pose a risk to National security, after review procedures set forth in EO 12968 have been exercised.

Derivative Classification - The incorporating, paraphrasing, restating or generating, in new form, information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification direction. The duplication or reproduction of existing classified information is not derivative classification.

Designated Approving Authority (DAA) - Official who formally assumes responsibility for operating an ITS or network at an acceptable level of risk.

Designated Country (Foreign National) - Citizen of a Foreign Country to which the United States has no official diplomatic relationship due to the country having ties to or sponsors terrorists, nuclear proliferation concerns, missile technology concerns, or is engaged in supporting the illegal trafficking in arms or drugs, or both.

Downgrading - the authorized reduction of the classification category of information to a lower classification category.

Duress Alarm - A mechanical or electronic device that enables threatened personnel to alert a response force in order to obtain immediate assistance without arousing the suspicion of the perpetrator.

Escort - The management of a visitor's movements and/or accesses implemented through the constant presence and monitoring of the visitor by appropriately designated and properly trained U.S. Government or approved contractor personnel. Training shall include the purpose of the visit, where the individual may access the Center, where the individual may go, whom the individual is to meet, authorized topics of discussion, etc.

Executive Order (EO) - Official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government.

Foreign National - Foreign National - For the purpose of general security protection, considerations of national security, and access accountability: Any person who is not a citizen of the United States. Includes lawful permanent resident (i.e., holders of green cards) or persons admitted with refugee status to the United States. See definition of Lawful Permanent Resident (LPR) in this Chapter.

Foreign Person - Any person who is not a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is not a protected individual as defined by 8 U.S.C. 1324b(a)(3). Also means any foreign corporation, business association, partnerships, trust, society or any other eneitity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions).

Formerly Restricted Data (FRD) - Information developed by the Department of Energy (DOE) related to National Nuclear programs with strict access restrictions "Restricted Data (RD)" but that has subsequently been downgraded to a lower level of control and accountability.

Grant Recipient - Organization (Universities, nonprofits, etc.) or individual that has received official designation and funding to perform specific research on behalf of NASA.

High Risk Position - Any position whose duties involve responsibilities and authorities that if misused can reasonably be expected to cause exceptionally serious adverse impact on NASA's mission.

HRO - Human Resources Office.

Information Technology System (ITS) - An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

Intergovernmental Personnel Act (IPA) - Individuals on temporary assignments between Federal agencies and State, local, and Indian Tribal Governments, institutions of higher education, and other eligible organizations. Can include Foreign Nationals.

Infrastructure - A collection of assets. See definitions for asset and system.

IT-1 Position - Any IT position whose duties, responsibilities, and authorities involve accessing information or system controls that if misused can reasonably be expected to cause exceptionally serious adverse impact.

IT-2 Position - Any IT position whose duties, responsibilities, and authorities involve accessing information or systems that if misused can reasonably be expected to cause serious adverse impact or allow for great personal gain.

IT- 3 Position - Any other IT position whose duties, responsibilities, and authorities involve accessing information that if misused could reasonably be expected to have minimum adverse impact on the Agency's mission.

Integrity - The condition that exists when information is unchanged from its source and

has not been accidentally or intentionally modified, altered, or destroyed.

Intelligence Community - The aggregate of the following executive branch organizations and agencies involved in intelligence activities: the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the Department of State; intelligence elements of the military services; the Federal Bureau of Investigation; the Department of Homeland Security; the Department of the Treasury; the Department of Energy; and staff elements of the Office of the Director of Central Intelligence.

Interim Clearance - Temporary clearance granted; while awaiting completion of the completed investigation and issuance of final security clearance, as a result of a favorable review of submitted investigative forms.

Intermediate Use of Force - Term used to define an escalation in necessary force required to subdue a suspect that is between minimum force and deadly force.

International Partners - Foreign Nationals or U. S. citizen representatives of foreign governments, who are involved in a particular international program or project under an International Space Act Agreement (ISAA).

International Traffic in Arms Regulation (ITAR) - Regulations governing exports of national defense articles and national defense services (22 CFR Part 120).

Interdependency - Used in the context of the NASA mission essential infrastructure (MEI) protection program. Any asset that an MEI is dependent upon; NASA or other agency owned or operated that the MEI uses to perform its mission (e.g. power, communications, facility, other utilities, etc.) that if destroyed or otherwise interrupted could adversely impact the continued viability of the MEI asset.

Intrusion Detection System (IDS) - A security alarm which consists of one or more various types of components used to detect, assess, and notify of unauthorized access into a protected area.

Information Security Oversight Office (ISOO) - Office established under the Executive Office of the President (EOP) tasked with policy development and oversight of Federal agency compliance with National-level policy for management of CNSI.

Key Resources - Publicly or privately controlled resources essential to the minimal operations of the economy and government (Public Law 107-296, The Homeland Security Act, Section 2(9)). Key resources include such facilities as nuclear power plants, dams, government facilities, and commercial facilities.

Lautenberg Ammendment - The Lautenberg Amendment to the Gun Control Act of 1968 became effective 30 September 1996. The Lautenberg Amendment makes it a felony for anyone convicted of a misdemeanor crime of "domestic violence" (e.g., assault or attempted assault on a family member) to ship, transport, possess, or receive firearms or ammunition. There is no exception for law enforcement or security personnel engaged in official duties. The Amendment also makes it a felony for anyone to sell or issue a firearm or ammunition to a person with such a conviction. This includes NASA personnel and contractors who furnish weapons or ammunition to persons knowing, or having reason to believe, they have qualifying convictions.

Lawful Permanent Resident (LPR) - Replaces the term "Permanent Resident Alien (PRA)" - A non-U.S. citizen, legally permitted to reside and work within the United States and issued the Resident Alien Identification (Green Card). Afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the Federal sector (except for specific needs or under temporary appointments per 5 CFR, Part 7, Section 7.4), and access to classified national security information. (NOTE: LPR's are not prohibited from accessing export controlled commodities but must still have a work related "need-to-know" and are still considered Foreign Nationals under immigration laws.)

Level of IDS Protection - Number of sensor types used in an IDS system to protect an area, i.e., door switches and motion detectors in use in one area constitute two levels of protection.

Lawful Permanent Resident (LPR) - Replaces the term "Permanent Resident Alien (PRA)" - A non-U.S. citizen, legally permitted to reside and work within the United States and issued the Resident Alien Identification (Green Card). Afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the Federal sector (except for specific needs or under temporary appointments per 5 CFR, Part 7, Section 7.4), and access to classified national security information. (NOTE: LPR's are not prohibited from accessing export controlled commodities but must still have a work related "need-to-know" and are still considered Foreign Nationals under immigration laws. See definitions for Foreign National, Foreign Persons, and U.S. Persons in this chapter).

Likelihood of Aggressor Activity - A determination by qualified security, law enforcement, and intelligence professionals, based on thorough knowledge and evaluation of intelligence data, that an "aggressor" is or is not likely to be interested in compromising a NASA asset.

Limited Area - A space in which security measures are applied primarily for the safeguarding of classified information and material or unclassified property warranting special protection and in which the uncontrolled movement of visitors would permit access to such classified information and material or property. But within such space, access shall be prevented by appropriate visitor escort and other internal restrictions and controls.

Limited Background Investigation (LBI) - The LBI consists of a personal subject interview, a basic National Agency Check (NAC) including a credit search, personnel interviews with employment, residence (neighbors), and educational sources, and law enforcement searches. Coverage is for a 3-year period while record searches are for a 5-year period. The MBI or LBI may be conducted for Moderate Risk positions.

Local Records Check (LRC) - Process of checking with local law enforcement agencies and courthouses for the purpose of obtaining, substantiating, or refuting information related to an individual(s) undergoing a background investigation.

Limited Privileged Access - Granted to a user to use system-level commands and files to bypass security controls for part of a system.

Low Risk Position - Any position whose duties involve responsibilities and authorities that if misused could reasonably be expected to have limited to no adverse impact on the Agency's mission.

Mandatory Declassification Review - The review for declassification of cl , ass , ifi , ed information in response to a request for declassification that meets the requirements under PART 3 of EO 12958.

Minimum Background Investigation (MBI) - The MBI consists of a personal subject interview, a basic National Agency Check (NAC), and a credit search covering a 5-year period. The MBI or LBI may be conducted for Moderate Risk positions.

Mission-Critical Space Program Personnel Reliability Program - Any Personnel Reliability Program (PRP) status and duties, which, if performed by employees in a faulty, negligent, or malicious manner, could jeopardize mission-critical space systems and delay a mission.

Mission-Essential Infrastructure (MEI) - Key resources/assets that the Agency depends upon to perform and maintain its most essential missions and operations. These resources may include critical components and facilities associated with the Space Shuttle, expendable launch vehicles, associated upper stages, Spacelab, International Space Station, command communication and control capability, Government-owned flight or experimental flight vehicles and apparatus, and one-of-a-kind irreplaceable facilities.

Mission Essential Infrastructure Protection Program (MEIPP) - The planning and implementation , of an enhanced protection level for Agency key resources identified by an NASA organization to be so crucial to the success of NASA missions as to warrant protection over that which would be routinely provided to NASA assets.

Moderate Risk Position - Any position whose duties involve responsibilities and authorities that if misused can reasonably be expected to cause moderate adverse impact on NASA's mission.

NASA Employee - NASA Civil Service personnel.

NASA-Controlled Facility - NASA Centers and individual facilities where access is c , ontrolled by issuance and mandatory use of photo-identification badges, armed security force personnel, and electronic access control systems to ensure only authorized personnel are admitted.

NASA PHOTO-ID - refers to the NASA photo-ID that has any number of imbedded and external technology capable of activating any type of facility, IT, or personal recognition access control system. Technology shall include: Exterior bar code and magnetic stripe embedded proximity chip, and embedded "smart card" chip.

NASA National Agency Check - Conducted electronically by NASA Security Offices of the files of the Federal Bureau of Investigation (including fingerprint files), Office of Defense Central Index of Investigations (DCII), the Office of Personnel Management, or other Government agencies, as appropriate. The files of the Bureau of Immigration and Customs Enforcement (BICE), the Central Intelligence Agency, and the U.S. State Department shall be reviewed, as available, when the individual is a resident alien or naturalized citizen of the United States.

National Agency Check (NAC) - The NAC is a search of the following four indices:

(1) U.S. Office of Personnel Management (U.S. OPM) Security/Suitability Investigations Index (SII) contains investigations completed by U.S. OPM and by other Federal agencies.

(2) Federal Bureau of Investigation (FBI) Identification Division (FBIF) contains a fingerprint index and name file.

(3) FBI Records Management Division (FBIN) contains files and records of all other investigations (e.g., background, criminal, loyalty, intelligence); and

(4) Defense Clearance and Investigations Index (DCII) contains investigations, including criminal investigations, conducted on civilian and military personnel in the Department of Defense.

(Note: The NAC is not a background investigation. It is one of the components that make up a background investigation.)

National Agency Check and Inquiries (NACI) - The NACI is a NAC that also includes written inquiries sent to employers, educational sources, law enforcement agencies, and references. The NACI is the minimum acceptable investigation for access to government facilities.

National Security Positions - Positions that have the potential to cause damage to the national security. These positions require access to classified information and are designated by the level of potential damage to the national security:

(1) **Confidential** - Information, the unauthorized disclosure of which reasonably could be expected to cause damage to National security that the Original Classification Authority (OCA) is able to identify or describe.

(2) **Secret** - Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to National security that the OCA is able to identify or describe.

(3) **Top Secret** - Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to National security that the OCA is able to identify or describe.

Need to Know - An administrative determination made by the authorized holder of classified information, that a prospective recipient has the requisite security clearance and requires access to specific classified information in order to perform or assist in lawful and authorized Governmental functions.

Noncritical Sensitive (NCS) (EO 10450) - One of the three levels for designating national security-related positions and the degree of risk involved. Includes any position involving access to Secret or Confidential information.

Non-deadly Physical Force - Pursuant to a lawful arrest by a security force officer, only that physical force which is reasonable and necessary to apprehend and arrest the offender; to prevent the escape of the offender; or to defend himself, herself or a third person from what is reasonably believed to be the use or threat of imminent use of non-deadly physical force by the offender. Verbal abuse alone by an offender cannot be the basis under any circumstances for the use of non-deadly physical force.

Nondesignated Country - Country with which the United States has favorable diplomatic relations.

Nondisclosure Agreement - Generally in the form of an SF 112 (Nondisclosure Form)

signed by the individual receiving a security clearance or given access to CNSI that acknowledges responsibility to share information of a classified nature only with personnel possessing the appropriate clearance and a demonstrable need-to-know.

Non-NASA Employee - Any individual, (e.g., other Federal Agency Civil Service personnel on detail to NASA, contractor, grantee, research associate) who is not a NASA Civil Service employee.

Nonsensitive Position Designation -

Nonsensitive Position Designation - Any NASA position that does not require access to CNSI.

Open Storage - Storage of CNSI in a security vault or strong room that does not incorporate secondary level storage in security containers.

Ordinary Force - A degree of force that is neither likely nor intended to cause death or great harm.

Original Classification Authority (OCA) - An individual authorized in writing, either by the President or by agency heads or other senior Government officials designated by the President, to classify information in the first instance.

Periodic Reinvestigation (PRI) - The PRI consists of a National Agency Check, a credit search, a Personal Subject Interview, selected record searches (e.g., law enforcement, personnel security files, and official personnel files (OPF)). Coverage is for a 5-year period. A PRI is required for all High Risk positions.

Permanent Resident Alien (PRA) - A non-U.S. citizen, legally permitted to reside and work within the United States and issued the Resident Alien Identification (Green Card). Afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the Federal sector (except for specific needs or under temporary appointments per 5 CFR, Part 7, Section 7.4), and access to classified national security information. (NOTE: PRA's are not prohibited from accessing export controlled commodities but must still have a work related "need-to-know" and are still considered Foreign Nationals under immigration laws.)

Presidential Decision Directive - Official documents whereby the President of the United States promulgates Presidential decisions on national security matters.

Personal Subject Interview (PRSI) - A Personal Subject Interview is an essential element of a background investigation and provides the subject of an investigation the opportunity to update, clarify, and explain information on their investigative questionnaire.

Physical Security Vulnerability Risk Assessment - A formal review, conducted by security professionals, that evaluates the physical security posture of an asset to assist in determining the overall security vulnerability of the asset.

"Private" NASA IT System - Those NASA IT systems to which access is restricted and appropriately controlled through a formal process. Granting of access is contingent upon a favorable security background investigation commensurate with the risk level of the system.

Privileged Access - That which is granted to a user so that files, processes, and system

commands are readable, writable, executable, and/or transferable. This allows a user to bypass security controls.

Protected Persons - A non-U.S. citizen allowed into the country under "refugee," "displaced person," "religious," or "political" persecution status.

"Public" NASA IT System - Those NASA IT systems to which access is unrestricted.

Public Trust Positions - Public Trust Positions have the potential for affecting the integrity, efficiency, and/or effectiveness of NASA's mission, and when breached, diminishes public confidence. Classic public trust positions include law enforcement and public safety and health. Positions with responsibility for managing programs or operations require a high degree of public trust because of their ability to significantly affect the accomplishment of NASA's mission.

Public Trust Position Designations - The designations of positions indicat **e** the potential for action or inaction by the incumbent of the position to affect the integrity, efficiency, and effectiveness of Government operations. Public trust risk designations are used in conjunction with security clearance requirements to determine the investigative requirements for the position. Positions involving high degrees of public trust, e.g., those with broad policy making authority or fiduciary responsibilities, trigger a more thorough investigation than do positions requiring only the finding that an applicant or an incumbent has the requisite stability of character to hold Federal employment. The three public trust risk designation levels are high, moderate, and low.

a. HIGH RISK: A position that has potential for exceptionally serious impact involving duties especially critical to the **A** gency or a program mission of the **A** gency with broad scope of policy or program authority such as:

(1) **P** olicy development and implementation;

(2) **H** igher level management assignments;

(3) **I** ndependent spokespersons or non-management positions with authority for independent action;

(4) **S** ignificant involvement in life-critical or mission critical systems; or

(5) **R** elatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization of disbursement from systems of dollar amounts of $10 million per year or greater, or lesser amounts if the activities of the individual are not subject to technical review by higher authority to ensure the integrity of the system.

(6) **P** ositions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for the direction and control of risk analysis and/or threat assessment, planning, and design of the computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with the relatively high risk for causing grave damage or realize a significant personal gain;

b. MODERATE RISK: A position that has the potential for moderate to serious impact involving duties of considerable importance to the **A** gency or a program mission of the **A** gency with significant program responsibilities and delivery of customer services to the public such as:

(1) **A** ssistants to policy development and implementation;

(2) **M** id-level management assignments;

(3) **N** on-management positions with authority for independent or semiindependent action;

(4) **D** elivery of service positions that demand public confidence or trust; or

(5) **P** ositions with responsibility for the direction, planning, design, operation, or maintenance of a computer system and whose work is technically reviewed by a higher authority at the high risk level to ensure the integrity of the system. Such positions may include but are not limited to:

(a) **A** ccess to and/or processing of sensitive but unclassified information and/or data, including, but not limited to: proprietary data, Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;

(b) **A** ccounting, disbursement, or authorization for disbursement from systems of dollar amounts of less than $10 million per year; or

(c) **O** ther positions as designated by the **A** gency head that involve degree of access to a system that creates a significant potential for damage or personal gain less than that in high risk positions.

c. LOW RISK: Positions that have the potential for impact involving duties of limited relation to the **A** gency mission with program responsibilities which affect the efficiency of the service. It also refers to those positions that do not fall within the definition of a high or moderate risk position.

Reasonable Force - Only that force necessary to overcome an opposing force.

Reimbursable Suitability/Security Investigation (RSI) - The RSI is a concentrated investigation to obtain additional information to resolve issues or to establish a history or pattern of behavior.

Reliability - Term used to denote contractor employee fitness for unescorted access to NASA Centers, facilities, and information technology. Determined by the conduct of a background investigation appropriate for the risk level of the position to be occupied.

Restricted Area - A space in which security measures are applied to safeguard or control property or to protect operations and functions that are vital or essential to the accomplishment of the mission assigned to a Center or Component Facility.

Restricted Data (RD) - Data developed by the Department of Energy (DOE) with extremely strict access restrictions.

Revocation - The removal of an individual's eligibility to access classified information based upon an adjudication that continued access to classified information poses a risk to national security and after review procedures set forth in EO 12968 have been exercised.

Risk Acceptance - An official acknowledgement by a management officials that they accept the risk posed by not implementing a recommendation, or requirement, designed to reduce or mitigate the risk.

Risk Acceptance Authority (RAA) - An individual designated in writing who makes the final determination on waivers to security standards and requirements when a security

deficiency has been determined to pose a serious risk to a program.

Risk Assessment - A formal process whereby a project, program, or event is evaluated to determine the types and level of risk associated with its implementation.

Risk Management - A means whereby NASA management implements select measures designed to reduce or mitigate known risks.

Security Adjudication Review Panel (SARP) - A group of senior management officials designated by the AA/OSPP who are responsible for assessing and determining the appropriateness of a removal or denial of a security clearance.

Security Clearance - A designation identifying an individual's highest level of allowable access to classified information based upon a positive adjudication that the individual does not pose a risk to National security.

Security Survey - A comprehensive formal evaluation of a facility, area, or activity by security specialists to determine its physical or technical strengths and weaknesses and to propose recommendations for improvement.

Security Violation - an act or action by an individual or individual(s) that is in conflict with NASA security policy or procedure (e.g., loss or compromise of CNSI; refusal to properly display NASA Photo-ID; violation of escort policy; security area violations, etc.). (NOTE: Does not include incidents of criminal activity; e.g., theft, assault, Dui, etc.)

Senior Management Official - Agency or Center management personnel at Division Chief or higher level.

Sensitive Compartmented Information (SCI) - Classification level denoting information, generally intelligence related, requiring security clearances and physical/procedural security measures above those established for collateral classified information or SAP information.

Sensitive But Unclassified (SBU) Controlled Information/Material - Unclassified information or material determined to have special protection requirements to preclude unauthorized disclosure to avoid compromises, risks to facilities, projects or programs, threat to the security and/or safety of the source of information, or to meet access restrictions established by laws, directives, or regulations:

(1) ITAR - International Traffic in Arms Regulations
(2) EAR - Export Administration Regulations
(3) MCTL - Militarily Critical Technologies List
(4) FAR - Federal Acquisition Regulations
(5) Privacy Act
(6) Proprietary
(7) FOIA - Freedom of Information Act
(8) UCNI - Unclassified Controlled Nuclear Information
(9) NASA Developed Software
(10) Scientific and Technical Information (STI)
(11) Source Selection and Bid and Proposal Information
(12) Inventions

Significant Adverse Impact - An act or occurrence that results in a negative outcome and/or damage/destruction of an asset, program, mission, or operation thereby delaying, interrupting, or prohibiting performance and mission accomplishment for an unspecified

period of time.

Single Scope Background Investigation (SSBI) - The SSBI consists of a Personal Subject Interview, National Agency Check, credit search, personal interviews of sources, written inquiries, and record searches, which cover specific areas of the subject's background during the past 10 years.

Special Access Program (SAP) - Any program established and approved under EO 12958 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

Special Security Office - Organization responsible for managing security programs related to special access and SCI operations.

Special Sensitive (SS) (EO 10450) - One of the three sensitivity levels for designating National security-related positions and the degree of risk involved, including any position that the head of the Agency determines to be in a level higher than Critical-Sensitive because of the greater degree of damage that an individual, by virtue of occupancy of the position, could cause to the National security or because of investigative requirements for this position under authority other than EO 10450 (e.g., NSD 61 which standardizes the scope and coverage for all investigations conducted for access to Collateral Top Secret/National Security Information, and Sensitive Compartmented Information).

Strong Room - Any room within a NASA building that has been modified to meet minimum construction and physical security standards for storage of CNSI. Generally established for "open storage" of CNSI.

Subject Matter Expert (SME) - An individual who possesses in-depth, expert knowledge of a program, process, technology, or information sufficient to establish classification caveats or determine the need or appropriateness of an existing national security classification.

Suitability - Refers to identifiable character traits and past conduct which are sufficient to determine whether a given individual is or is not likely to be able to carry out the duties of a Federal job. Suitability is distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, skills, and abilities.

Suspension - The temporary removal of an individual's access to classified information, pending the completion of an investigation and final adjudication.

System Security Engineering - A process established to identify and incorporate security provisions as early as possible in program or project system designs, acquisitions, or modifications, thereby minimizing costs, vulnerabilities, and compromises.

Systematic Review for Declassification - The review for declassification of CNSI contained in records that have been determined by the Archivist of the United States to have permanent historical value in accordance with the requirements under PART 3, Section 3.4 of EO 12958.

TEMPEST - An unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term "compromising emanations" which are unintentional emissions that could disclose

information being transmitted, received, or handled by any automated information processing equipment.

TEMPEST Test - A laboratory or onsite (field) examination to determine the nature and amplitude of conducted or radiated signals containing compromising information, which normally includes detection and measurement of these signals and analysis to determine correlation between received signals, and potentially compromising transmitted signals.

Technical Surveillance - Covert installation or modification of equipment to monitor (visually or audibly) activities within target areas or to acquire information by specialized means.

Technical Surveillance Countermeasures (TSCM) - The means taken to prevent, detect, and neutralize efforts to acquire information by technical surveillance.

Temporary Eligibility for Access - Based on a justified need that meets the requirements of EO 12968, temporary access to CNSI shall be granted before investigations are complete and favorably adjudicated when official functions must be performed prior to completion of the investigation and adjudication process. See Apendix C: SPB Issuance 1-97.

Threat Assessment - A formal, in-depth review and evaluation of the capabilities and interests of identified aggressors for the purpose of determining their potential for targeting NASA operations and assets.

TSCM Surveys and Inspections - A thorough physical, electronic, and visual examination to detect surveillance devices, technical security hazards, and attempts at clandestine penetration of an area for hostile collection of information.

Update Investigations - (LDI - Update of Previous LBI Completed, BDI - Update of Previous BI Completed, SDI - Update of Previous SSBI Completed). These investigations are conducted due to break in service or to fulfill Agency requirements. They consist of the same coverage as the prior investigation (LBI, BI, and SSBI) from 13 to 60 months of the previous investigation's closing date. (Update LBI=LDI, updated BI=BDI, and updated SSBI=SDI.)

Upgrade Investigations - (BGI - Upgrade to BI from LBI Completed, LGI -Upgrade to LBI from an MBI Completed, SGI - Upgrade to SSBI from BI Completed). These investigations are conducted when there is a change in an employee's position risk level form a lower to a higher sensitivity designation. These investigations provide the proper coverage for the level of investigation currently required and also take into account the scope of the previous investigation. This investigation is for movement upward in sensitivity and covers the period form 0 to 60 months of the previous investigation's closing date. (BGI=LBI to BI, LGI=MBI to LBI, SGI=BI to SSBI.)

Unauthorized disclosure (EO 12958) - A communication or physical transfer of classified information to a recipient who does not have the appropriate credentials for access.

UNCI (Unclassified Controlled Nuclear Information) - Sensitive unclassified Government information concerning nuclear material, weapons, and components, whose dissemination is controlled under Section 148, of the Atomic Energy Act

Uncleared Person - An individual who does not possess a security clearance. This makes them ineligible to access CNSI.

Unreasonable use of Force - Use of force in excess of the degree required to overcome resistance.

Unsupervised environment - (Used in the context of NASA child-care providers) An environment within or outside a NASA Childcare Center that provides for no direct continuous observation of an uninvestigated child-care worker by a properly investigated employee. Observation may take the form of direct personal participation or through video surveillance.

Use of Force Report - A written report, submitted by the arresting officer and supervisor, used to document details of the force used to lawfully subdue an individual.

U.S. Person (non-U.S. Citizen) - For the purpose of implementing protection and accountability under the ITAR; A person who is a lawful permanent resident (LPR) as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do bus , iness in the United , States. It also includes any governmental (federal, state, or local) entity. It does not include any foreign person as defined in this chapter.

Vulnerability Risk Assessment - A formal evaluation, conducted by security professionals, of a critical asset's (e.g., facility, person, equipment, aircraft, spacecraft) risk from theft, sabotage, death, or destruction, resulting in a determination of level of vulnerability and subsequent development and implementation of security measures (physical and procedur , al) designed to negate or eliminate those vulnerabilities.

Waiver - The approved continuance of a condition authorized by the AA/OSPP that varies from a requirement and implements risk management on the designated vulnerability.

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS